

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-030146

(43)Date of publication of application : 31.01.2003

(51)Int.Cl.

G06F 15/00

G06F 13/00

H04L 9/32

H04Q 7/38

(21)Application number : 2001-217376

(71)Applicant : NEC CORP

(22)Date of filing : 17.07.2001

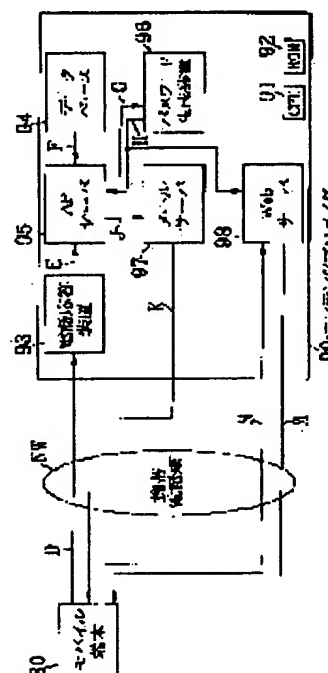
(72)Inventor : UEJIMA YOSHIYUKI

(54) NETWORK SYSTEM WITH TERMINAL AUTHENTICATING FUNCTION, AND TERMINAL AUTHENTICATING METHOD AND AUTHENTICATION CONTROL PROGRAM USED FOR THE SAME SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a network system with a terminal authenticating function which can perform authentication with high security through easy operation.

SOLUTION: A user calls a contents provider 90 through a user terminal 80. The contents provider 90 recognizes the telephone number E of the mobile terminal 80 which has made the call and confirms that the mobile terminal 80 is registered as a member by performing retrieval from a database 94, and then send mail K including a password for allowing access to the telephone number E. The mobile terminal 80 accesses a Web server 98 by using a URL with a one-time password, so a user who is not allowed to access the Web server 98 is unable to access the server and the security can be made high.



LEGAL STATUS

[Date of request for examination]

12.06.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-30146

(P2003-30146A)

(43)公開日 平成15年1月31日(2003.1.31)

(51)Int.Cl. ⁷	識別記号	F I	テ-マ-コ-ト*(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 8 5
13/00	6 1 0	13/00	6 1 0 S 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 B 5 K 0 6 7
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R

審査請求 有 請求項の数13 O L (全 12 頁)

(21)出願番号 特願2001-217376(P2001-217376)

(22)出願日 平成13年7月17日(2001.7.17)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 上島 良之

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100099830

弁理士 西村 征生

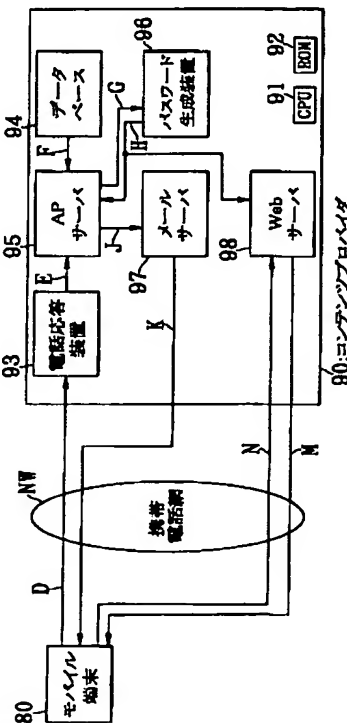
最終頁に続く

(54)【発明の名称】 端末認証機能を有するネットワークシステム、該システムに用いられる端末認証方法及び認証制御プログラム

(57)【要約】

【課題】 簡単な操作でセキュリティの高い認証ができる端末認証機能を有するネットワークシステムを提供する。

【解決手段】 ユーザは、モバイル端末80からコンテンツプロバイダ90に対して電話をかける。コンテンツプロバイダ90は、電話をかけてきたモバイル端末80の電話番号Eを認識し、データベース94を検索して同モバイル端末80がユーザ登録されていることを確認した後、電話番号E宛にアクセスを許可するためのパスワードを含むメールKを送信する。モバイル端末80は、Webサーバ98に対してワンタイムパスワード付きのURLを用いてアクセスを行うので、アクセスを許可されていないユーザが同Webサーバ98にアクセスすることは不可能であり、セキュリティを高くすることができる。



【特許請求の範囲】

【請求項 1】 ユーザ端末と、コンテンツプロバイダとを備えてなるネットワークシステムにおいて、前記ユーザ端末が自端末の第 1 のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行い、前記コンテンツプロバイダが前記発呼信号を受信して該発呼信号に含まれる前記第 1 のネットワークアドレスを抽出し、契約しているユーザの第 2 のネットワークアドレスと前記第 1 のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワードを生成して登録すると共に該パスワードを含む URL (Uniform Resource Locator) を記述したメールを前記第 1 のネットワークアドレスを用いて前記ユーザ端末へ送信し、前記ユーザ端末から前記 URL を含むアクセス要求情報を受信したとき、該 URL に含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給することを特徴とする端末認証方法。

【請求項 2】 ユーザ端末と、コンテンツプロバイダとを備えてなるネットワークシステムにおいて、前記ユーザ端末が自端末の第 1 のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行い、前記コンテンツプロバイダが、前記発呼信号を受信して該発呼信号に含まれる前記第 1 のネットワークアドレスを抽出する応答処理と、契約しているユーザの第 2 のネットワークアドレスと前記第 1 のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワード生成指示信号及びメール送信指示信号を生成する指示信号生成処理と、前記パスワード生成指示信号に基づいてパスワードを生成するパスワード生成処理と、前記メール送信指示信号に基づいて前記パスワードを含む URL を記述したメールを前記第 1 のネットワークアドレスを用いて前記ユーザ端末へ送信するメール送信処理と、前記パスワード生成処理で生成された前記パスワードを登録すると共に、前記ユーザ端末から前記 URL を含むアクセス要求情報を受信したとき、該 URL に含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給するアクセス許可処理とを行うことを特徴とする端末認証方法。

【請求項 3】 ユーザ端末と、コンテンツプロバイダとを備えてなるネットワークシステムにおいて、

前記ユーザ端末が自端末の第 1 のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行い、前記コンテンツプロバイダが前記発呼信号を受信して該発呼信号に含まれる前記第 1 のネットワークアドレスを抽出し、契約しているユーザの第 2 のネットワークアドレスと前記第 1 のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワードを生成して登録すると共に該パスワードを含む URL を記述したメールを前記第 1 のネットワークアドレスを用いて前記ユーザ端末へ送信し、前記ユーザ端末から前記 URL を含むアクセス要求情報を受信したとき、該 URL に含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に固有の端末符号を送信し、該端末符号と前記ユーザ端末から送信された端末符号とを比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給することを特徴とする端末認証方法。

【請求項 4】 ユーザ端末と、コンテンツプロバイダとを備えてなるネットワークシステムにおいて、前記ユーザ端末が自端末の第 1 のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行い、前記コンテンツプロバイダが、前記発呼信号を受信して該発呼信号に含まれる前記第 1 のネットワークアドレスを抽出する応答処理と、契約しているユーザの第 2 のネットワークアドレスと前記第 1 のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワード生成指示信号及びメール送信指示信号を生成する指示信号生成処理と、前記パスワード生成指示信号に基づいてパスワードを生成するパスワード生成処理と、前記メール送信指示信号に基づいて前記パスワードを含む URL を記述したメールを前記第 1 のネットワークアドレスを用いて前記ユーザ端末へ送信するメール送信処理と、前記ユーザ端末毎に固有の端末符号を生成する端末符号生成処理と、前記パスワード生成処理で生成された前記パスワードを登録すると共に、前記ユーザ端末から前記 URL を含むアクセス要求情報を受信したとき、該 URL に含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に該当の前記端末符号を送信し、該端末符号と前記ユーザ端末から送信された端末符号とを比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツ

を供給するアクセス許可処理とを行うことを特徴とする端末認証方法。

【請求項 5】 前記パスワードは、ワンタイムパスワードであることを特徴とする請求項 1、2、3 又は 4 記載の端末認証方法。

【請求項 6】 前記第 1 のネットワークアドレスは、前記ユーザ端末の電話番号であることを特徴とする請求項 1、2、3、4 又は 5 記載の端末認証方法。

【請求項 7】 ユーザ端末と、コンテンツプロバイダとを備え、端末認証機能を有するネットワークシステムであって、

前記ユーザ端末は、

自端末の第 1 のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行う構成とされ、

前記コンテンツプロバイダは、

前記発呼信号を受信して該発呼信号に含まれる前記第 1 のネットワークアドレスを抽出し、契約しているユーザの第 2 のネットワークアドレスと前記第 1 のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワードを生成して登録すると共に該パスワードを含む URL を記述したメールを前記第 1 のネットワークアドレスを用いて前記ユーザ端末へ送信し、前記ユーザ端末から前記 URL を含むアクセス要求情報を受信したとき、該 URL に含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給する構成とされていることを特徴とするネットワークシステム。

【請求項 8】 前記コンテンツプロバイダは、前記発呼信号を受信して該発呼信号に含まれる前記第 1 のネットワークアドレスを抽出する応答装置と、契約しているユーザの第 2 のネットワークアドレスを予め保持するデータベースと、

前記第 1 のネットワークアドレスと前記第 2 のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワード生成指示信号及びメール送信指示信号を生成するアクセスポイントサーバと、

前記パスワード生成指示信号に基づいてパスワードを生成するパスワード生成装置と、

前記メール送信指示信号に基づいて前記パスワードを含む URL を記述したメールを前記第 1 のネットワークアドレスを用いて前記ユーザ端末へ送信するメールサーバと、

前記パスワード生成装置で生成された前記パスワードを登録すると共に、前記ユーザ端末から前記 URL を含むアクセス要求情報を受信したとき、該 URL に含まれた前記パスワードを前記登録されているパスワードと比較

し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給するコンテンツサーバとで構成されていることを特徴とする請求項 7 記載のネットワークシステム。

【請求項 9】 ユーザ端末と、コンテンツプロバイダとを備え、端末認証機能を有するネットワークシステムであって、

前記ユーザ端末は、

自端末の第 1 のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行う構成とされ、

前記コンテンツプロバイダは、

前記発呼信号を受信して該発呼信号に含まれる前記第 1 のネットワークアドレスを抽出し、契約しているユーザの第 2 のネットワークアドレスと前記第 1 のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワードを生成して登録すると共に該パスワードを含む URL を記述したメールを前記第 1 のネットワークアドレスを用いて前記ユーザ端末へ送信し、前記ユーザ端末から前記 URL を含むアクセス要求情報を受信したとき、該 URL に含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に固有の端末符号を送信し、該端末符号と前記ユーザ端末から送信された端末符号とを比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給する構成とされていることを特徴とするネットワークシステム。

【請求項 10】 前記コンテンツプロバイダは、前記発呼信号を受信して該発呼信号に含まれる前記第 1 のネットワークアドレスを抽出する応答装置と、契約しているユーザの第 2 のネットワークアドレスを予め保持するデータベースと、

前記第 1 のネットワークアドレスと前記第 2 のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワード生成指示信号及びメール送信指示信号を生成するアクセスポイントサーバと、

前記パスワード生成指示信号に基づいてパスワードを生成するパスワード生成装置と、

前記メール送信指示信号に基づいて前記パスワードを含む URL を記述したメールを前記第 1 のネットワークアドレスを用いて前記ユーザ端末へ送信するメールサーバと、

前記ユーザ端末毎に固有の端末符号を生成する端末符号生成装置と、

前記パスワード生成装置で生成された前記パスワードを登録すると共に、前記ユーザ端末から前記 URL を含むアクセス要求情報を受信したとき、該 URL に含まれた前記パスワードを前記登録されているパスワードと比較

5

し、一致しているときに前記ユーザ端末に該当の前記端末符号を送信し、該端末符号と前記ユーザ端末から送信された端末符号とを比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給するコンテンツサーバとで構成されていることを特徴とする請求項9記載のネットワークシステム。

【請求項11】 前記パスワードは、ワンタイムパスワードであることを特徴とする請求項7、8、9又は10記載のネットワークシステム。

【請求項12】 前記第1のネットワークアドレスは、前記ユーザ端末の電話番号であることを特徴とする請求項7、8、9、10又は11記載のネットワークシステム。

【請求項13】 コンピュータに請求項7、8、9、10、11又は12記載のネットワークシステムの機能を実現させるための認証制御プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、端末認証機能を有するネットワークシステム、該システムに用いられる端末認証方法及び認証制御プログラムに係り、特に、高度のセキュリティを必要とする場合に用いて好適な端末認証機能を有するネットワークシステム、該システムに用いられる端末認証方法及び認証制御プログラムに関する。

【0002】

【従来の技術】携帯電話機などのユーザ端末をLAN（ローカル・エリア・ネットワーク）やインターネットなどを介してコンテンツプロバイダに接続する場合、従来の端末認証方法では、ユーザ端末から電話番号を含む発呼信号が出力されたとき、この電話番号がユーザIDに変換され、同ユーザIDが予め登録されたものと一致したときに接続が許可されるようになっている。

【0003】この種の端末認証方法に用いるネットワークシステムは、従来では例えば図5に示すように、モバイル端末10と、通信キャリア20と、コンテンツプロバイダ30とで構成されている。モバイル端末10は、例えば携帯電話機などのユーザ端末であり、ユーザの操作に基づいて電話番号を含む発呼信号Aを生成する。通信キャリア20は、発呼信号Aに含まれた電話番号をユーザID情報Bに変換する変換サーバ21を有すると共に、コンテンツプロバイダ30から提供されたコンテンツCをモバイル端末10へ送信する。コンテンツプロバイダ30は、コンテンツサーバ31を有し、ユーザID情報Bを入力して予め登録されたIDと比較することによりモバイル端末10を認証し、この認証後にコンテンツCを出力する。

【0004】このネットワークシステムでは、モバイル端末10から発呼信号Aが出力され、同発呼信号Aに含まれた電話番号が変換サーバ21でユーザID情報Bに

6

変換される。ユーザID情報Bは、コンテンツサーバ31に入力されて予め登録されたIDと比較され、一致したときにモバイル端末10の接続が許可される。その後、モバイル端末10から要求されたコンテンツCが通信キャリア20を経て同モバイル端末10へ送信される。

【0005】ところが、何らかの方法でユーザID情報Bが第三者に入手された場合、同第三者がユーザ本人になりすましてモバイル端末10をコンテンツプロバイダ30に容易に接続できるという問題があった。

【0006】この問題を解決するために、例えば、文献；特開2001-45562号公報に記載された端末認証システムが提案されている。図6は、前記文献に記載された端末認証システムの構成図である。この端末認証システムは、同図に示すように、携帯電話機41と、固定電話機42と、ファクシミリ（以下、「FAX」という）43と、ページャ44と、パーソナルコンピュータ45と、携帯電話通信網46と、公衆回線網47と、無線呼出網48と、インターネット49と、公衆回線網接続部50と、データベース60と、メールサーバ71と、パスワード発行部72と、パスワード管理部73と、ネットワーク74と、認証システム部75とで構成されている。

【0007】この端末認証システムでは、ユーザUは、携帯電話機41又は固定電話機42を用いてパスワードの発行及び送信をパスワード発行部72に要求する。このように、ユーザUがパスワードの発行を要求するとき用いる電話機をパスワード発行要求端末という。パスワード発行要求端末として使用できる端末は、端末自体が電話番号を有するものであり、携帯電話機41、固定電話機42の他、PHS（Personal Handy phone System）端末、FAXに付属の電話機、電話機能を備える携帯情報端末（Personal Digital Assistants、PDA）、及びモデムやターミナルアダプタが接続されたパーソナルコンピュータなどがある。

【0008】一方、ユーザUがパスワード発行部72からパスワードを受け取る場合、携帯電話機41や固定電話機42を介して音声情報として受け取るが、同携帯電話機41や同固定電話機42に画像表示部があれば、同画像表示部に文字情報で表示して受け取っても良い。又、パスワードは、ファクシミリ装置43、ページャ44、パーソナルコンピュータ45で受信することもできる。このように、ユーザUがパスワードを受信するために用いる端末を、パスワード受信端末という。認証システム部75には、パスワード発行部72からパスワードが送出されて保持されている。ユーザUは、パスワード受信端末で受信したパスワードを携帯電話機41や固定電話機42（パスワード発行要求端末）を介して認証システム部75に入力する。そして、認証システム部75で、ユーザUがパスワード発行部72から受け取ったパスワードと、同認証システム部75が同パスワード発行

部 7 2 から受け取ったパスワードとが比較されて最終的に認証が行われる。

【0009】

【発明が解決しようとする課題】しかしながら、図 6 に記載された端末認証システムでは、次のような問題点があった。すなわち、ユーザ U は、携帯電話機 4 1、固定電話機 4 2、FAX 4 3、ページャ 4 4、パーソナルコンピュータ 4 5 などを利用して、テキスト、バイナリ、音声、画像などの形式でパスワードを入手することができるが、パスワード発行要求端末とパスワード受信端末とが異なる場合、受け取ったパスワードをパスワード発行要求端末に入力する過程で、パスワードの漏洩など、セキュリティ上の問題が発生する。又、パスワード発行要求端末とパスワード受信端末とが同一のものである場合でも、パスワードを入力し直す必要があるため、ユーザにとって利便性が悪いという問題があった。

【0010】この発明は、上述の事情に鑑みてなされたもので、ユーザの操作が簡単で、かつセキュリティの高い認証ができる端末認証機能を有するネットワークシステム、該システムに用いられる端末認証方法及び認証制御プログラムを提供することを目的としている。

【0011】

【課題を解決するための手段】上記課題を解決するために、請求項 1 記載の発明は、端末認証方法に係り、ユーザ端末と、コンテンツプロバイダとを備えてなるネットワークシステムにおいて、前記ユーザ端末が自端末の第 1 のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行い、前記コンテンツプロバイダが前記発呼信号を受信して該発呼信号に含まれる前記第 1 のネットワークアドレスを抽出し、契約しているユーザの第 2 のネットワークアドレスと前記第 1 のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワードを生成して登録すると共に該パスワードを含む URL

(Uniform Resource Locator) を記述したメールを前記第 1 のネットワークアドレスを用いて前記ユーザ端末へ送信し、前記ユーザ端末から前記 URL を含むアクセス要求情報を受信したとき、該 URL に含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給することを特徴としている。

【0012】請求項 2 記載の発明は、端末認証方法に係り、ユーザ端末と、コンテンツプロバイダとを備えてなるネットワークシステムにおいて、前記ユーザ端末が自端末の第 1 のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メール

に含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行い、前記コンテンツプロバイダが、前記発呼信号を受信して該発呼信号に含まれる前記第 1 のネットワークアドレスを抽出する応答処理と、契約しているユーザの第 2 のネットワークアドレスと前記第 1 のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワード生成指示信号及びメール送信指示信号を生成する指示信号生成処理と、前記パスワード生成指示信号に基づいてパスワードを生成するパスワード生成処理と、前記メール送信指示信号に基づいて前記パスワードを含む URL を記述したメールを前記第 1 のネットワークアドレスを用いて前記ユーザ端末へ送信するメール送信処理と、前記パスワード生成処理で生成された前記パスワードを登録すると共に、前記ユーザ端末から前記 URL を含むアクセス要求情報を受信したとき、該 URL に含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給するアクセス許可処理とを行うことを特徴としている。

【0013】請求項 3 記載の発明は、端末認証方法に係り、ユーザ端末と、コンテンツプロバイダとを備えてなるネットワークシステムにおいて、前記ユーザ端末が自端末の第 1 のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行い、前記コンテンツプロバイダが前記発呼信号を受信して該発呼信号に含まれる前記第 1 のネットワークアドレスを抽出し、契約しているユーザの第 2 のネットワークアドレスと前記第 1 のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワードを生成して登録すると共に該パスワードを含む URL を記述したメールを前記第 1 のネットワークアドレスを用いて前記ユーザ端末へ送信し、前記ユーザ端末から前記 URL を含むアクセス要求情報を受信したとき、該 URL に含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に固有の端末符号を送信し、該端末符号と前記ユーザ端末から送信された端末符号とを比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給することを特徴としている。

【0014】請求項 4 記載の発明は、端末認証方法に係り、ユーザ端末と、コンテンツプロバイダとを備えてなるネットワークシステムにおいて、前記ユーザ端末が自端末の第 1 のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行い、前記コンテンツプロバイダが、前

記発呼信号を受信して該発呼信号に含まれる前記第1のネットワークアドレスを抽出する応答処理と、契約しているユーザの第2のネットワークアドレスと前記第1のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワード生成指示信号及びメール送信指示信号を生成する指示信号生成処理と、前記パスワード生成指示信号に基づいてパスワードを生成するパスワード生成処理と、前記メール送信指示信号に基づいて前記パスワードを含むURLを記述したメールを前記第1のネットワークアドレスを用いて前記ユーザ端末へ送信するメール送信処理と、前記ユーザ端末毎に固有の端末符号を生成する端末符号生成処理と、前記パスワード生成処理で生成された前記パスワードを登録すると共に、前記ユーザ端末から前記URLを含むアクセス要求情報を受信したとき、該URLに含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に該当の前記端末符号を送信し、該端末符号と前記ユーザ端末から送信された端末符号とを比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給するアクセス許可処理とを行うことを特徴としている。

【0015】請求項5記載の発明は、請求項1、2、3又は4記載の端末認証方法に係り、前記パスワードは、ワンタイムパスワードであることを特徴としている。

【0016】請求項6記載の発明は、請求項1、2、3、4又は5記載の端末認証方法に係り、前記第1のネットワークアドレスは、前記ユーザ端末の電話番号であることを特徴としている。

【0017】請求項7記載の発明は、ユーザ端末と、コンテンツプロバイダとを備え、端末認証機能を有するネットワークシステムに係り、前記ユーザ端末は、自端末の第1のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行う構成とされ、前記コンテンツプロバイダは、前記発呼信号を受信して該発呼信号に含まれる前記第1のネットワークアドレスを抽出し、契約しているユーザの第2のネットワークアドレスと前記第1のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワードを生成して登録すると共に該パスワードを含むURLを記述したメールを前記第1のネットワークアドレスを用いて前記ユーザ端末へ送信し、前記ユーザ端末から前記URLを含むアクセス要求情報を受信したとき、該URLに含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給する構成とされていることを特徴としている。

【0018】請求項8記載の発明は、請求項7記載のネ

ットワークシステムに係り、前記コンテンツプロバイダは、前記発呼信号を受信して該発呼信号に含まれる前記第1のネットワークアドレスを抽出する応答装置と、契約しているユーザの第2のネットワークアドレスを予め保持するデータベースと、前記第1のネットワークアドレスと前記第2のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワード生成指示信号及びメール送信指示信号を生成するアクセスポイントサーバと、前記パスワード生成指示信号に基づいてパスワードを生成するパスワード生成装置と、前記メール送信指示信号に基づいて前記パスワードを含むURLを記述したメールを前記第1のネットワークアドレスを用いて前記ユーザ端末へ送信するメールサーバと、前記パスワード生成装置で生成された前記パスワードを登録すると共に、前記ユーザ端末から前記URLを含むアクセス要求情報を受信したとき、該URLに含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給するコンテンツサーバとで構成されていることを特徴としている。

【0019】請求項9記載の発明は、ユーザ端末と、コンテンツプロバイダとを備え、端末認証機能を有するネットワークシステムに係り、前記ユーザ端末は、自端末の第1のネットワークアドレスを含む発呼信号を生成して前記コンテンツプロバイダへ送信すると共に、前記コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いて前記コンテンツプロバイダにアクセスを行う構成とされ、前記コンテンツプロバイダは、前記発呼信号を受信して該発呼信号に含まれる前記第1のネットワークアドレスを抽出し、契約しているユーザの第2のネットワークアドレスと前記第1のネットワークアドレスとを比較して前記ユーザ端末を認証したとき、パスワードを生成して登録すると共に該パスワードを含むURLを記述したメールを前記第1のネットワークアドレスを用いて前記ユーザ端末へ送信し、前記ユーザ端末から前記URLを含むアクセス要求情報を受信したとき、該URLに含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に固有の端末符号を送信し、該端末符号と前記ユーザ端末から送信された端末符号とを比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給する構成とされていることを特徴としている。

【0020】請求項10記載の発明は、請求項9記載のネットワークシステムに係り、前記コンテンツプロバイダは、前記発呼信号を受信して該発呼信号に含まれる前記第1のネットワークアドレスを抽出する応答装置と、契約しているユーザの第2のネットワークアドレスを予め保持するデータベースと、前記第1のネットワークアドレスと前記第2のネットワークアドレスとを比較して

前記ユーザ端末を認証したとき、パスワード生成指示信号及びメール送信指示信号を生成するアクセスポイントサーバと、前記パスワード生成指示信号に基づいてパスワードを生成するパスワード生成装置と、前記メール送信指示信号に基づいて前記パスワードを含むURLを記述したメールを前記第1のネットワークアドレスを用いて前記ユーザ端末へ送信するメールサーバと、前記ユーザ端末毎に固有の端末符号を生成する端末符号生成装置と、前記パスワード生成装置で生成された前記パスワードを登録すると共に、前記ユーザ端末から前記URLを含むアクセス要求情報を受信したとき、該URLに含まれた前記パスワードを前記登録されているパスワードと比較し、一致しているときに前記ユーザ端末に該当の前記端末符号を送信し、該端末符号と前記ユーザ端末から送信された端末符号とを比較し、一致しているときに前記ユーザ端末に対してアクセスを許可して所定のコンテンツを供給するコンテンツサーバとで構成されていることを特徴としている。

【0021】請求項1記載の発明は、請求項7、8、9又は10記載のネットワークシステムに係り、前記パスワードは、ワンタイムパスワードであることを特徴としている。

【0022】請求項12記載の発明は、請求項7、8、9、10又は11記載のネットワークシステムに係り、前記第1のネットワークアドレスは、前記ユーザ端末の電話番号であることを特徴としている。

【0023】請求項13記載の発明は、認証制御プログラムに係り、コンピュータに請求項7、8、9、10、11又は12記載のネットワークシステムの機能を実現させることを特徴としている。

【0024】

【発明の実施の形態】以下、図面を参照して、この発明の実施の形態について説明する。

第1の実施形態

図1は、この発明の第1の実施形態である端末認証方法を実施するためのネットワークシステムの構成を示すブロック図である。この形態のネットワークシステムは、同図に示すように、モバイル端末（即ち、ユーザ端末）80と、コンテンツプロバイダ90とで構成されている。モバイル端末80は、例えば携帯電話機などで構成され、自端末の電話番号（即ち、第1のネットワークアドレス）を含む発呼信号Dを生成してコンテンツプロバイダ90へ送信すると共に、同コンテンツプロバイダからメールKを受信して同メールKに含まれたパスワードを用いて同コンテンツプロバイダ90にアクセスを行う。

【0025】コンテンツプロバイダ90は、例えば、コンテンツ供給企業などに設置されている情報処理装置であり、同コンテンツプロバイダ90全体を制御する中央処理装置（以下、「CPU」という）91及び同CPU

91を動作させるための認証制御プログラムが記録された記録媒体（例えば、リード・オンリ・メモリ、以下、「ROM」という）92を有している。さらに、コンテンツプロバイダ90は、電話応答装置（即ち、応答装置）93と、データベース94と、アクセスポイントサーバ（以下、「APサーバ」という）95と、パスワード生成装置96と、メールサーバ97と、Webサーバ（即ち、コンテンツサーバ）98とを備えている。電話応答装置93は、携帯電話網NWを介して発呼信号Dを受信して同発呼信号Dに含まれる電話番号Eを抽出し、同携帯電話網NWと接続状態を遮断する。

【0026】データベース94は、契約しているユーザの電話番号（即ち、第2のネットワークアドレス）Fを予め保持する。APサーバ95は、電話番号Eと電話番号Fとを比較してモバイル端末80を認証したとき、パスワード生成指示信号G及びメール送信指示信号Jを生成する。パスワード生成装置96は、パスワード生成指示信号Gに基づいて、パスワードHを生成する。パスワードHは、Webサーバ98に対してアクセスが1回のみの可能なワンタイムパスワードである。メールサーバ97は、メール送信指示信号Jに基づいて、パスワードHを含むURLを記述したメールKを電話番号Eを用いてモバイル端末80へ送信する。このメールKに記述されたURLは、例えば、

http://Webサーバのアドレス/index.htm?passwd=xxxxxxx

xx
で表される。パスワード“xxxxxxx”の部分は、パスワード生成装置96によって生成されたパスワードHである。

【0027】Webサーバ98は、パスワードHを登録すると共に、モバイル端末80から前記URLを含むアクセス要求情報Nを受信したとき、同URLに含まれたパスワードHを同Webサーバ98に登録されているパスワードと比較し、一致しているときにモバイル端末80に対してアクセスを許可して同モバイル端末80から要求されたコンテンツMを供給する。また、Webサーバ98は、URLにパスワードが含まれていない場合、含まれているパスワードが1度使用されている場合、又は含まれているパスワードが誤っている場合には、モバイル端末80に対してアクセスを許可しない。さらに、Webサーバ98は、モバイル端末80からURLを受信し、このURLが指定するWeb画面データを同モバイル端末80に送信する。また、Webサーバ98は、Web画面データの中にあるリンク先のURL全てにパスワード生成装置96で生成されたパスワードHを付加した形で、Web画面データを生成する。

【0028】また、モバイル端末80は、ユーザを限定したWebサーバ98へアクセスするとき、電話番号を通知する方法で電話をかけ、同Webサーバ98に対するアクセスを許可するパスワード付きのURLを受け取

るとき、電話番号を利用したメールアドレス（例えば、“090xxxxxxxx@xxxxxx.ne.jp”）宛のメールを受信し、指定された同パスワード付きのURLでWebサーバ98にアクセスを行う。

【0029】図2及び図3は、図1のネットワークシステムの動作を説明するためのフローチャートである。これらの図2及び図3を参照して、この形態の端末認証方法の処理内容について説明する。ユーザの操作に基づいてモバイル端末80から電話応答装置93に対して発呼が行われる（ステップA1）。電話応答装置93は、着呼に対して自動応答し（ステップA2、応答処理）、着呼時に通知される電話番号Eを受信し（ステップA3）、携帯電話網NWと遮断する（ステップA4）。電話応答装置93は、電話番号EをAPサーバ95へ通知する（ステップA5）。APサーバ95は、データベース94にアクセスし、モバイル端末80のユーザを検索する（ステップA6）。次に、APサーバ95は、電話応答装置93から得た電話番号Eとデータベース94の情報（即ち、電話番号F）との比較を行う（ステップA7）。比較の結果、モバイル端末80の電話番号Eがデータベース94に予め登録されているユーザの電話番号Fと一致しない場合（NG）、処理が終了する。

【0030】一方、電話をかけてきたモバイル端末80の電話番号Eが登録されていることが確認された場合（OK）、APサーバ95は、パスワード生成装置96にパスワード生成指示信号Gを送出する（指示信号生成処理）。パスワード生成装置96は、1回だけ使用することが有効なパスワードH（ワンタイムパスワード）を生成し（ステップA8、パスワード生成処理）、APサーバ95とWebサーバ98とに同パスワードHのデータを送出する。APサーバ95は、パスワードHのデータを受け取り、メールサーバ97にメール送信指示信号Jを送出する（ステップA9）。このとき、APサーバ95からメールサーバ97には、メールの送信先となる電話番号、メールの本文に記述されるパスワード、Webサーバ98へアクセスするためのURLが通知される。

【0031】メールサーバ97は、メール送信指示信号Jを受け取り、APサーバ95より受け取った電話番号、パスワード、URLの情報をもとにメールを組み立て、電話番号をメールアドレスとする宛先にURLとパスワードを組み合わせたWebサーバ98へのアクセス先を本文に記述し、モバイル端末80に対してメールKを送信する（ステップA10、メール送信処理）。モバイル端末80は、メールKを受信する（ステップA11）。受信したメールKには、Webサーバ98へアクセスするためのURLが記述されているので、モバイル端末80は、このURLを利用してWebサーバ98へアクセス要求情報Nを送出してアクセス要求を行う（ステップA12）。一般的に、Webサーバ98へアクセ

ス可能な携帯電話機などでは、メールの本文に記述されたURL部分を選択した状態にして実行することにより、容易に同Webサーバ98へのアクセスが実行される。

【0032】Webサーバ98は、アクセス要求情報Nを受け取り、URLに付加されているパスワードHを抽出し（ステップA13）、アクセスを許可するか否かの判定を行う（ステップA14）。判定の結果、URLにパスワードが付加されていない場合、付加されているパスワードが1度使用されている場合、及び付加されているパスワードが誤っている場合には、Webサーバ98へのアクセスは許可せずに、アクセス拒否のWeb画面をモバイル端末80に送信し、処理を終了する（END）。

【0033】一方、Webサーバ98は、モバイル端末80から送られてきたパスワードが、パスワード生成装置96から通知されたパスワードHと一致していることを確認した場合、Webサーバ98へのアクセスを許可する（OK、アクセス許可処理）。Webサーバ98は、アクセスを許可した場合、モバイル端末80に対して送信するWeb画面データのリンク先のURL全てに、パスワード生成装置96が生成したパスワードHを付加してWeb画面データを生成する（ステップA15）。Webサーバ98は、生成したWeb画面データをモバイル端末80に送信する（ステップA16）。

【0034】モバイル端末80は、Webサーバ98から送信されたWeb画面データを受信すると、同Web画面データをもとに画面を表示する（ステップA17）。モバイル端末80は、画面に表示されているリンク先のURLを使って再度Webサーバ98にアクセスするとき、リンク先のURLにパスワードHが付加されているので、パスワード付きのURLをWebサーバ98に送信する（ステップA18）。以後、Webサーバ98は、モバイル端末80から受信したURLに付加されているパスワードを判定し、パスワードが正しければWeb画面データを送信する処理を繰り返す。また、Webサーバ98は、モバイル端末80の要求に基づいてコンテンツMを供給する。

【0035】以上のように、この第1の実施形態では、ユーザは、モバイル端末80からユーザIDやパスワードを入力する必要がなく、電話をかける操作のみを行えば良いので、同ユーザの操作が簡単になる。さらに、コンテンツプロバイダ90は、電話をかけてきたモバイル端末80の電話番号Eを認識し、ユーザ登録されていることを確認した後、電話番号E宛にアクセスを許可するためのパスワードを含むメールKを送信するので、ユーザ端末を円滑に特定できる。その上、モバイル端末80は、Webサーバ98に対してワンタイムパスワード付きのURLを用いてアクセスを行うので、アクセスを許可されていないユーザが同Webサーバ98にアクセス

することは不可能であり、セキュリティを高くすることができる。

【0036】第2の実施形態

図4は、この発明の第2の実施形態である端末認証方法を実施するためのネットワークシステムの構成を示すブロック図であり、第1の実施形態を示す図1中の要素と共通の要素には共通の符号が付されている。この形態のネットワークシステムでは、同図に示すように、図1中のコンテンツプロバイダ90に代えて、新たな機能が付加されたコンテンツプロバイダ90Aが設けられている。コンテンツプロバイダ90Aでは、コンテンツプロバイダ90の構成に加え、端末符号生成装置99が新たに設けられると共に、図1中のWebサーバ98に代えて、新たな機能が付加されたWebサーバ98Aが設けられている。端末符号生成装置99は、コンテンツプロバイダ90Aに携帯電話網NWなどネットワークを介して接続されたモバイル端末80などのユーザ端末毎に、固有の端末符号Nを生成する。

【0037】Webサーバ98Aは、パスワード生成装置96で生成されたパスワードHを登録すると共に、モバイル端末80などのユーザ端末からURLを含むアクセス要求情報を受信したとき、同URLに含まれたパスワードHをWebサーバ98Aに登録されているパスワードと比較し、一致しているときに同ユーザ端末に該当の端末符号NをURLの末尾に付加した形式でページを生成して送信し、同端末符号Nと同ユーザ端末から送信された端末符号とを比較し、一致しているときに同ユーザ端末に対してアクセスを許可して同モバイル端末80から要求されたコンテンツMを供給する。他は、図1と同様の構成である。

【0038】この形態の端末認証方法では、次の点が第1の実施形態の処理内容と異なっている。すなわち、モバイル端末80がパスワードHによって認証された後（図3中のステップA14）、Webサーバ98Aは、端末符号生成装置99で生成された端末符号NをURLの末尾に付加した形式でユーザ毎にページを生成し、モバイル端末80にWebページデータを送信する。モバイル端末80は、このWebページデータを、第三者に読み出しが不可能な形式（例えば、i-mode（登録商標）の画面メモ）で記録する。この場合、例えば、ブックマーク（Bookmark）などのように、アドレスが直接表示されたり、第三者によって読み出しができるような形式は、記録したページのアドレスが読み出されるので、使用できない。

【0039】Webページデータがモバイル端末80に記録された後、同モバイル端末80は、記録したページへアクセスする。このとき、Webサーバ98Aに送信されるアドレスには、端末符号Nが付加されている。Webサーバ98Aは、この端末符号Nを用いてモバイル端末80の認証を行い、アクセスの可否を判定する。モ

バイル端末80からWebサーバ98Aへ電話をかけてパスワードHを得るアクセスは、初回のみで良く、2回目以降のアクセスは、画面メモなどに記録されたページを読み出すことによって行われる。

【0040】以上のように、この第2の実施形態では、Webサーバ98Aは、端末符号Nを用いてモバイル端末80を認証し、かつ同モバイル端末80は、自端末に記録したページへアクセスするのみでWebサーバ98Aを利用できるので、第1の実施形態の利点に加え、さらに簡単な操作でアクセスが行われると共に、セキュリティを高めることができる。

【0041】以上、この発明の実施形態を図面により詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計の変更などがあってもこの発明に含まれる。例えば、図1及び図4では、APサーバ95、メールサーバ97、データベース94、パスワード生成装置96、Webサーバ98、98A、及び端末符号生成装置99は、分割されたブロックで構成されているが、1台から複数台のハードウェアで構成することが可能である。また、図1及び図4では、モバイル端末80とコンテンツプロバイダ90、90Aとは、携帯電話網NWを介して接続されているが、携帯電話網NWに限らず、例えば、LAN（ローカル・エリア・ネットワーク）やインターネットなど、任意の通信回線で良い。

【0042】

【発明の効果】以上説明したように、この発明の構成によれば、ユーザは、ユーザ端末からユーザIDやパスワードを入力する必要がなく、電話をかける操作のみを行えば良いので、同ユーザの操作を簡単にできる。さらに、コンテンツプロバイダは、電話をかけてきたユーザ端末の電話番号を認識し、ユーザ登録されていることを確認した後、同電話番号のユーザ端末宛にアクセスを許可するためのパスワードを含むメールを送信するので、ユーザ端末を円滑に特定できる。その上、ユーザ端末は、コンテンツサーバに対してワンタイムパスワード付きのURLを用いてアクセスを行うので、アクセスを許可されていないユーザが同コンテンツサーバにアクセスすることは不可能であり、セキュリティを高くすることができる。また、コンテンツサーバは、端末符号を用いてユーザ端末を認証し、かつ同ユーザ端末は、自端末に記録したページへアクセスするのみでコンテンツサーバを利用できるので、さらに簡単な操作でアクセスが行われると共に、セキュリティを高めることができる。

【図面の簡単な説明】

【図1】この発明の第1の実施形態である端末認証方法を実施するためのネットワークシステムの構成を示すブロック図である。

【図2】図1のネットワークシステムの動作を説明するためのフローチャートである。

17

18

【図3】図1のネットワークシステムの動作を説明するためのフローチャートである。

【図4】この発明の第2の実施形態である端末認証方法を実施するためのネットワークシステムの構成を示すブロック図である。

【図5】従来の端末認証方法に用いるネットワークシステムの構成を示すブロック図である。

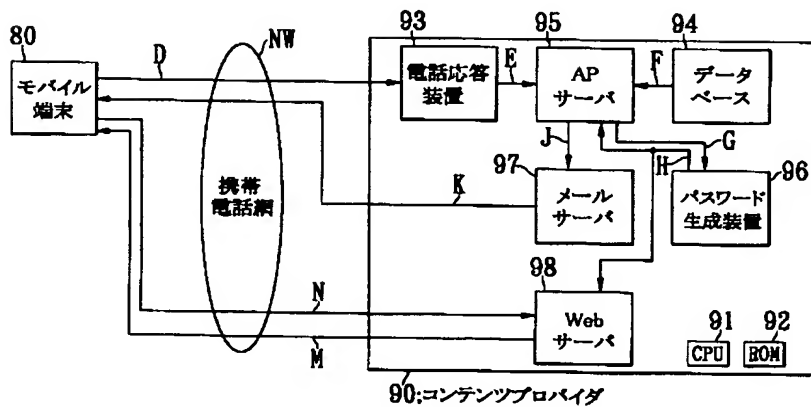
【図6】従来の端末認証システムの構成図である。

【符号の説明】

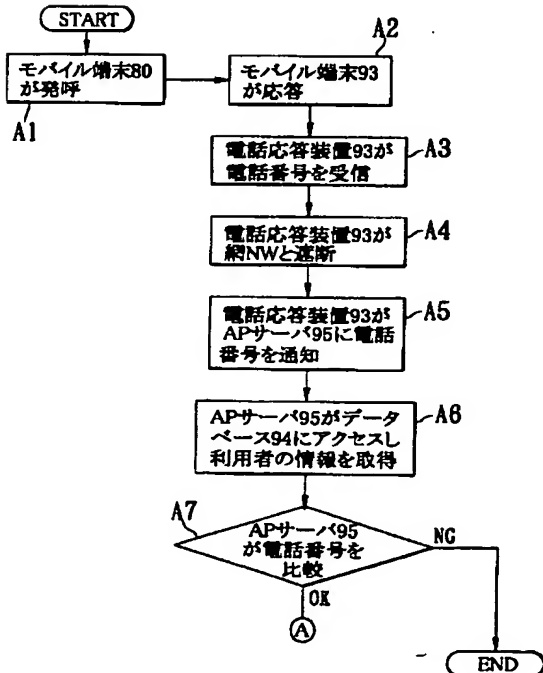
80 モバイル端末 (ユーザ端末)

10

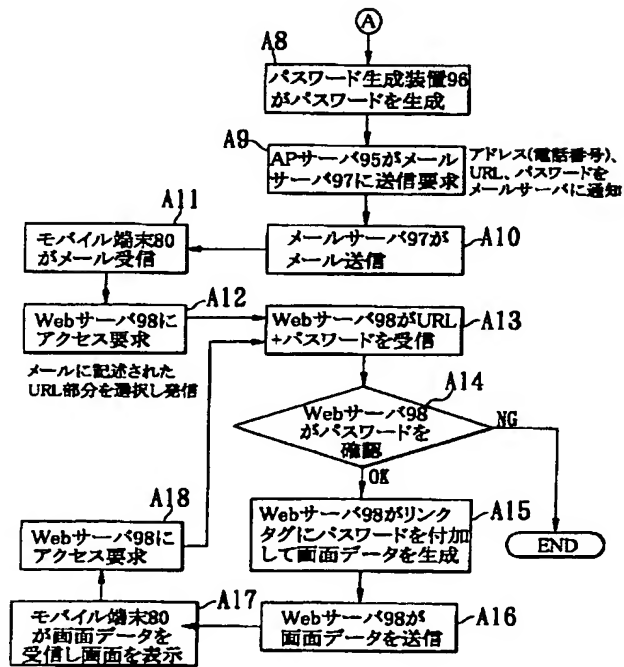
【図1】



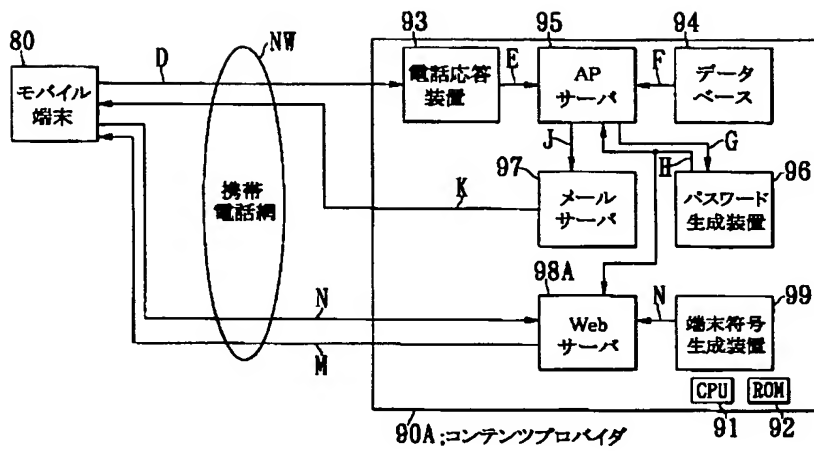
【図2】



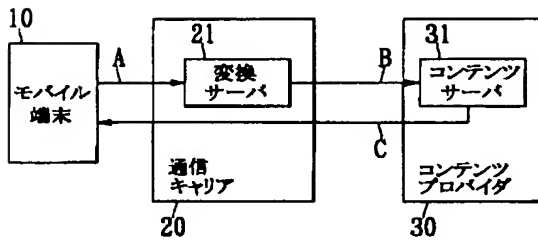
【図3】



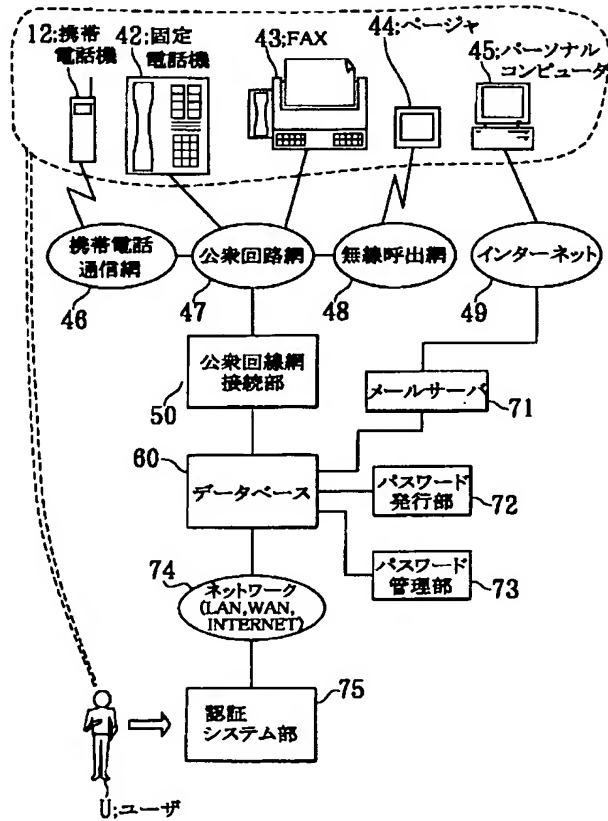
【図 4】



【図 5】



【図 6】



フロントページの続き

Fターム(参考) 5B085 AE02 AE03 BC02

5J104 AA07 AA16 EA01 EA03 EA16

KA02 KA21 NA05 PA07

5K067 AA30 AA34 BB04 DD16 DD17

EE02 EE10 EE16 HH22 HH23

KK13 KK15